

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address)) Case No.23-985M(NJ)
Snapchat social media account)
"izayzay12" ("Subject Account"), as further)
described in Attachment A)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 8/24/2023 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

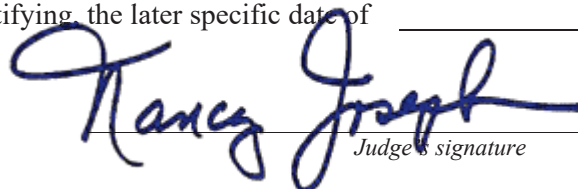
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____

Hon. Nancy Joseph
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 8/10/2023 @ 12:36 p.m.


Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

Property to Be Searched

Information associated with the Snapchat account having the username “izayzay12” (hereinafter “**Subject Account**”), which is stored at premises owned, maintained, controlled, or operated by Snapchat, Inc., located at 63 Market Street, Venice, California.

ATTACHMENT B

Particular Things to Be Seized

I. Search Procedure

1. In order to facilitate seizure by law enforcement of the records and information described in Attachment A, this affidavit and application for search warrant seek authorization, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to permit employees of Snapchat to assist agents in the execution of this warrant. In executing this warrant, the following procedures will be implemented.

2. The search warrant will be presented to Snapchat personnel, who will be directed to isolate those accounts and files described in Section II below.

3. In order to minimize any disruption of computer service to innocent third parties, company employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

4. Other Snapchat employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant.

5. Following the protocol set out in the Addendum to this Attachment, law enforcement personnel will thereafter review information and records received from company employees to locate the information to be seized by law enforcement personnel specified in Section III below.

II. Files and Accounts to be Copied by Snapchat Employees

To the extent that the information described below in Section III is within the possession, custody, or control of Snapchat, Snapchat is required to disclose the following information to the government:

a. all records or other information pertaining to the **Subject Account** including all files, databases, location information, and database records stored by Snapchat in relation to the listed account(s)

b. all information in the possession of Snapchat that might identify the subscribers related to this account or identifiers, including names, dates of birth, addresses, telephone numbers, email addresses, account creation date, the length of service (including start date), types of services utilized, timestamps and IP address for account logins/logouts, and means and source of payment for services (including any credit card or bank account number).

c. logs, including sender, recipient, date, time, message status (including if and when the message was opened), and whether the receiver used the native screen capture function of their device, concerning communications, including Snaps, Stories, or Chats, sent to or from **Subject Account**.

d. all information about which users of the **Subject Account** communicate with the most.

e. device information such as the model, operating system, operating system version, applications installed, mobile device phone number, equipment identifier (such as the Media Access Control (MAC) address, the International Mobile Equipment Identifier (IMEI), or

Mobile Equipment Identifier (MEID)), mobile network information of devices used by **Subject Account** in conjunction with the service.

f. contact lists or images Snapchat has obtained from devices used by the **Subject Account** respectively.

g. receipts for any transactions conducted by the **Subject Account** respectively.

h. content of all communications, including Snaps, Stories, or Chats, sent or received by **Subject Account**.

III. Information to be Seized by Law Enforcement Personnel

All information described above in Section II that constitutes evidence and instrumentalities of violations of Title 21, United States Code, Section 846 involving the **Subject Account**:

- a. Snapchat username;
- b. Email address;
- c. Phone number;
- d. Display name;
- e. Snapchat account creation date and IP address;
- f. Timestamp and IP address of account logins and logouts (may also include device information);
- g. Device information and device history;
- h. Purchase history (information about services and items purchased through Snap, including in-app purchases, custom filters, and lenses -- includes what was purchased and date of purchase);
- i. Account change history (a log of changes to the account made by the user, including dates/times of changes in registration email address or phone number, birthdate, and display name);
- j. Whether account phone number has been verified;
- k. Last Active date;
- l. Whether Maps is enabled;

- m. Whether two-factor-authentication is enabled;
- n. App version;
- o. Logs containing metadata about a user's Snaps, Stories, Chats;
- p. Associated accounts;
- q. Additional user profile data, including number of Stories viewed; "discover channels" viewed; and ads, apps, and websites that the user has interacted with;
- r. Subscriptions (the accounts/"discover channels" to which a user has "subscribed" (generally, content from brands, news organizations, corporate entities, or influencers));
- s. Friends (overview of the user's friends, the friend requests sent, and users blocked and deleted);
- t. Location data (for users who have turned on location service and opted into location services in the app settings) – including frequent locations, latest locations, top locations, and locations the user has visited;
- u. Memories content (until deleted by a user);
- v. Encrypted My Eyes Only content (Snap can provide the data file but cannot decrypt it);
- w. Search history;
- x. "Our Story" and Crowd-Sourced Content (content that the user submitted to Snap's curation team);
- y. Snap History (basic information about Snaps the user has recently sent and received, including the sender, recipient, type of Snap, and date). Because of Snap's retention policy, this information is likely to be extremely limited;
- z. Snap survey responses/results.

ADDENDUM TO ATTACHMENT B

With respect to the search of any information and records received from the social media company, law enforcement personnel will locate the information to be seized pursuant to Section III of Attachment B according to the following protocol.

The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. searching for and attempting to recover any hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein.
- b. surveying various file directories to determine whether they include data falling within the list of items to be seized as set forth herein.
- c. opening or reading portions of files and records, in order to determine whether their contents fall within the items to be seized as set forth herein, and/or
- d. performing key word searches through all records to determine whether occurrences of language contained in such records exist that are likely to appear in the information to be seized described in Section III of Attachment B.

Law enforcement personnel are not authorized to conduct additional searches on any information beyond the scope of the items to be seized by this warrant.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*Snapchat social media account "izayzay12" ("Subject
Account"), as further described in Attachment A

Case No. 23-985M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 21 U.S.C. §§ 841 & 846

Offense Description
 Distribution, and conspiracy to possess with the intent to distribute controlled substances.

The application is based on these facts:

See Attached Affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

THOMAS GROTH

Digitally signed by THOMAS GROTH
 Date: 2023.08.09 13:53:03 -05'00'

Applicant's signature

Thomas Groth, DEA SA

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
 _____ telephone _____ *(specify reliable electronic means).*

Date: 8/10/2023

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT
OF SNAPCHAT ACCOUNT

I, Thomas Groth, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent with DEA since July 2017. From March 2017 to July 2017, I attended and completed the DEA 20-week training academy in Quantico, Virginia. While at the DEA training academy, I received instruction in investigative techniques, drug identification, physical surveillance, undercover negotiations, telecommunication investigations, and drug-related law. I have also received on-the-job training from supervisors, senior agents, and detectives regarding the manner in which drugs are trafficked and money is laundered.

2. I am currently assigned to the DEA Chicago, Illinois Field Division, Milwaukee District Office (“DEA Milwaukee Office”). Within the DEA Milwaukee Office, I am assigned to an enforcement group targeting drug traffickers operating within the DEA Milwaukee Office’s area of responsibility. Prior to being assigned to the DEA Milwaukee Office, I was assigned to the DEA Phoenix, Arizona Field Division Office (“DEA Phoenix Office”) for approximately five and half years. Within the DEA Phoenix Office, I was in the Organized Crime Drug Enforcement Task Force (“OCDETF”)/Strike Force, Group One (“OCDETF SF1”). The OCDETF SF1 is tasked with disrupting and dismantling major drug-trafficking organizations through the collaborative investigative efforts of federal, state, and local law enforcement agencies.

3. Prior to being employed by the DEA, I was employed as a Police Officer with the Kenosha Police Department in Kenosha, Wisconsin for approximately five years. Before being hired by the Kenosha Police Department, I completed a 16-week training academy at the Great Oaks Police Academy in Cincinnati, Ohio.

4. I have a Bachelor of Science degree in Criminal Justice from Xavier University in Cincinnati, Ohio.

5. By virtue of my employment as a Special Agent and prior law enforcement experience, I have performed various tasks, which include, but are not limited to: (a) involvement in numerous investigations into illegal drug distribution conspiracies, participating in multiple arrests of individuals for drug related offenses, and participating in the service of multiple drug-related search warrants; (b) functioned as a surveillance agent, thus observing and recording movements of persons trafficking in drugs and those suspected of trafficking in drugs; (c) interviewed witnesses, confidential sources (CS) and sources of information (SOI) relative to the illegal trafficking of drugs and the distribution of monies and assets derived from the illegal trafficking of drugs (laundering of monetary instruments); (d) functioned as a case agent, entailing the supervision of specific investigations involving the trafficking of drugs; (e) and working with prosecutors to provide useful courtroom testimony.

6. In the course of conducting drug investigations, I have personally interviewed persons involved in the distribution of illegal drugs. I have become aware of techniques and practices used by narcotics traffickers to avoid detection by law enforcement. Among these techniques are the use of counter surveillance, multiple locations at which to conduct narcotics related activities, hidden compartments in vehicles used to conceal narcotics and currency, mobile telephones, voice mail, texting, instant messaging, email, encrypted applications, social media applications, various other applications and the use of numerous associates and “workers” to further their criminal organization. I have learned the various techniques individuals use to conceal the source or nature of drug proceeds. Among the techniques utilized are the purchase of assets

and financial instruments in nominee names using cash and “structuring” transactions so as to avoid certain reporting requirements of financial institutions.

7. This Affidavit is made in support of an application for a warrant to search the Snapchat¹ social media account “izayzay12” (“**Subject Account**”), which is further described below and in Attachment A to the Application, for evidence and instrumentalities, described further in Part III of Attachment B concerning narcotics offenses, in violation of Title 21, United States Code, Sections 841 and 846 (the “**Subject Offenses**”).

8. The statements in this Affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence and instrumentalities of violations of Title 21, United States Code, Sections 841 and 846 are located in the **Subject Account**.

Background on Snapchat

9. Based on my training and experience, and on information provided by Snapchat, Snapchat is one of the most popular applications for sending and receiving “self-destructing” messages, pictures, and videos. Snapchat is a messaging application for mobile phones with Apple’s iOS operating system and Google’s Android operating system. Snapchat offers four primary ways for users to communicate with each other: snaps, memories, stories, and chat.

¹ According to Snapchat’s law enforcement guide, its custodian of records is located at 63 Market Street, Venice, CA 90291. The guide is available at <https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf>.

10. **Snap.** A user takes a photo or video using their camera phone in real-time. The user then selects a time limit of 1-10 seconds for the receiver to view the photo or video. A user can elect to have the photo/video saved in their phone's photo gallery or just sent via Snapchat, without being saved. The photo/video can then be sent to a friend in Snapchat. The snap is deleted after the selected amount of time. If a recipient attempts to take a screenshot of the snap to save on his/her phone, the application will notify the sender of this behavior. Snapchat states that it deletes each snap from its servers once all recipients have viewed it. If a snap has not been viewed by all recipients, Snapchat states that it retains the snap for thirty days.

11. **Memories.** Memories is Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. A user can also edit and send Snaps and create Stories from these Memories. Snaps, Stories, and other photos and videos saved in Memories are backed up by Snapchat and may remain in Memories until deleted by the user.

12. **Stories.** A user can also add the photo/video Snap to their "Story." Depending on the user's privacy settings, the photos and videos added to a Story can be viewed by either all Snapchatters or just the user's friends for up to 24 hours. Stories can also be saved in Memories.

13. **Chat.** A user can also type messages to friends within the Snapchat app using the Chat feature. A user sends a Chat message to a friend, and once it is viewed by both parties – and both parties swipe away from the Chat screen – the message will be cleared. Within the Snapchat app itself, a user can opt to save part of the Chat by tapping on the message (text or photo) that he or she wants to keep. The user can clear the message by tapping it again. The Chat function also allows users to make live voice calls, which are similar to phone calls but occur through the

Snapchat application, and live video calls. Snapchat also obtains a variety of non-content information from its users.

14. **Usage Information.** Snapchat may collect information about how users interact with its services, including which search queries they submit, and how they communicate with other users, including maintaining a log of all snaps to and from an account for the last 31 days, for 24 hours of posted Stories, and for any unopened Chats or those saved by a sender or recipient, and how a user interacts with these messages (such as when a user opens a message).

15. **Device Information.** Snapchat collects information about the devices of its users, including information about the user's hardware and software, such as the hardware model, operating system version, device memory, advertising identifiers, unique application identifiers, apps installed, unique device identifiers, browser type, language, battery level, and time zone; information from device sensors, such as accelerometers, gyroscopes, compasses, microphones, and whether the user has headphones connected; and information about the user's wireless and mobile network connections, such as mobile phone number, service provider, and signal strength.

16. **Device Phonebook.** Snapchat may collection information about the phonebook of the user's device.

17. **Cameras and Photos.** Snapchat may collect images and other information from the user's device's camera and photos.

18. **Location Information.** Snapchat may collect information about the user's location, including precise location using methods that include GPS, wireless networks, cell towers, Wi-Fi access points, and other device sensors, such as gyroscopes, accelerometers, and compasses.

19. **Snap Map.** Snapchat allows a user to share location information with his/her friends and also obtain location information about the user's friends. Based on such information, Snapchat places the friends' locations on a map viewable to the user.

20. **Information Collected by Cookies and Other Technologies.** Snapchat may collect information through cookies and other technologies about the user's activity, browser, and device.

21. **Log Information.** Snapchat collects log information when a user uses Snapchat's website, including device information, access times, pages viewed, IP address, and pages visited.

Probable Cause

22. In June 2023, investigators met with a confidential source (CS-1) who had direct knowledge of Isaiah ALBRECHT-Facundo's (ALBRECHT-Facundo) drug trafficking activities. During the debriefing, CS-1 stated that ALBRECHT-Facundo currently sells multiple ounces of cocaine on a regular basis and believes ALBRECHT-Facundo obtains multiple kilograms of cocaine at a time. CS-1 stated that he/she communicates with ALBRECHT-Facundo through the Snapchat Application, in particular with ALBRECHT-Facundo's snapchat account "izayzay12" ("**Subject Account**").

23. CS-1 has been providing information to investigators since approximately June, 2023. CS-1 is providing information in exchange for consideration in potential future charges of possession with intent to distribute cocaine and carrying a concealed weapon. CS-1 is not being provided any monetary compensation. CS-1's criminal history includes convictions for disorderly conduct, misdemeanor bail jumping, criminal damage to property, and motor vehicle traffic offenses. The information provided by CS-1 was voluntarily provided against his/her

penal interests, has been independently corroborated and deemed accurate. As such investigators believe CS-1 to be truthful.

24. On June 27, 2023, CS-1 was in direct communication with ALBRECHT-Facundo through the Snapchat application in regard to obtaining cocaine later that same day. Investigators took pictures of their conversation. During the conversation, ALBRECHT-Facundo, utilizing the Snapchat display name “Facundo_” (Snapchat handle is “izayzay12” (**Subject Account**)), stated, among other things, “How fast you think you’re gonna move this one?” and “Can you just take 2 right now? Then if you need more I’ll get you more?”

25. Based on training and experience, investigators believe ALBRECHT-Facundo was negotiating with CS-1 concerning the quantity of drugs he was going to provide to CS-1 based on how fast CS-1 would “move” (sell) the units.

26. Following the aforementioned conversation via the **Subject Account**, investigators utilized CS-1 to conduct a controlled purchase from ALBRECHT-Facundo. The meeting was coordinated via the **Subject Account**. In particular, CS-1 purchased five ounces of cocaine from ALBRECHT-Facundo for \$4,000 in Kenosha, WI. Video and audio surveillance from the controlled purchase, along with CS-1 information, confirmed that ALBRECHT-Facundo provided the cocaine to CS-1. SIU Detectives later field tested a small sample of the suspected cocaine which resulted in a positive indication for cocaine. The total weight of the cocaine was 141.3 grams of cocaine.

Preservation of Snapchat Account “izayzay12”

27. In July 2023, based on the aforementioned information, investigators requested Snapchat preserve all information related to the **Subject Account**. Snapchat indicated they would

preserve the data for up to 90 days from the date of the preservation request related to the **Subject Account**.

Conclusion

28. In late June 2023, DEA and KPD SIU investigators conducted a controlled purchase of 5 ounces of cocaine from ALBRECHT-Facundo. Prior to the controlled purchase, ALBRECHT-Facundo was facilitating his drug trafficking activities via the Snapchat application, in particular the **Subject Account**. As a result, based upon the evidence set forth in this affidavit, there is probable cause to believe that the **Subject Account** has been used to facilitate the distribution, purchase, and possession of controlled substances. Likewise, based on CS information, I believe that ALBRECHT-Facundo is utilizing the **Subject Account** to communicate with numerous individuals involved in drug trafficking, not just the CS, and a search of the **Subject Account** will yield additional evidence of ALBRECHT-Facundo's involvement in drug trafficking.

29. Based on my training and experience in other investigations, I believe that a search of social network provider account contents often of individuals engaged in criminal conduct yields investigative leads relating to:

- a. the identities of suppliers, coconspirators, customers, and other individuals engaged in drug offenses;
- b. the contact information of suppliers, coconspirators, customers, and other individuals engaged in drug offenses;
- c. the timing of communications among suppliers, coconspirators, customers, and other individuals involved in drug offenses; and

- d. the methods and techniques used in drug offenses.

Search Procedure

30. In order to facilitate seizure by law enforcement of the records and information described in Attachment A, this affidavit and application for search warrant seek authorization, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to permit employees of Snapchat to assist agents in the execution of this warrant. In executing this warrant, the following procedures will be implemented:

- a. The search warrant will be presented to Snapchat personnel who will be directed to the information described in Section II of Attachment B;
- b. In order to minimize any disruption of computer service to innocent third parties, Snapchat employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II of Attachment B, including an exact duplicate of all information stored in the computer accounts and files described therein;
- c. Snapchat employees will provide the exact duplicate in electronic form of the information described in Section II of the Attachment B and all information stored in those accounts and files to the agent who serves this search warrant; and
- d. Following the protocol set out in the Addendum to Attachment B, law enforcement personnel will thereafter review all information and records received from Snapchat employees to locate the information to be seized by law enforcement personnel pursuant to Section III of Attachment B.

31. Based on the above information, I respectfully submit that there is probable cause to believe that evidence of violations of Title 21, United States Code, Section 846 are located in the Snapchat social media account “izayzay12” (hereinafter “**Subject Account**”), which are located within one or more computers and/or servers found at Snapchat, further described above and in Attachment A. By this affidavit and application, I request that the Court issue a search warrant directed to Snapchat allowing agents to seize the electronic evidence and other information stored on their servers following the search procedure described in Attachment B and the Addendum to Attachment B.

ATTACHMENT A

Property to Be Searched

Information associated with the Snapchat account having the username “izayzay12” (hereinafter “**Subject Account**”), which is stored at premises owned, maintained, controlled, or operated by Snapchat, Inc., located at 63 Market Street, Venice, California.

ATTACHMENT B

Particular Things to Be Seized

I. Search Procedure

1. In order to facilitate seizure by law enforcement of the records and information described in Attachment A, this affidavit and application for search warrant seek authorization, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to permit employees of Snapchat to assist agents in the execution of this warrant. In executing this warrant, the following procedures will be implemented.

2. The search warrant will be presented to Snapchat personnel, who will be directed to isolate those accounts and files described in Section II below.

3. In order to minimize any disruption of computer service to innocent third parties, company employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

4. Other Snapchat employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant.

5. Following the protocol set out in the Addendum to this Attachment, law enforcement personnel will thereafter review information and records received from company employees to locate the information to be seized by law enforcement personnel specified in Section III below.

II. Files and Accounts to be Copied by Snapchat Employees

To the extent that the information described below in Section III is within the possession, custody, or control of Snapchat, Snapchat is required to disclose the following information to the government:

- a. all records or other information pertaining to the **Subject Account** including all files, databases, location information, and database records stored by Snapchat in relation to the listed account(s)
- b. all information in the possession of Snapchat that might identify the subscribers related to this account or identifiers, including names, dates of birth, addresses, telephone numbers, email addresses, account creation date, the length of service (including start date), types of services utilized, timestamps and IP address for account logins/logouts, and means and source of payment for services (including any credit card or bank account number).
- c. logs, including sender, recipient, date, time, message status (including if and when the message was opened), and whether the receiver used the native screen capture function of their device, concerning communications, including Snaps, Stories, or Chats, sent to or from **Subject Account**.
- d. all information about which users of the **Subject Account** communicate with the most.
- e. device information such as the model, operating system, operating system version, applications installed, mobile device phone number, equipment identifier (such as the Media Access Control (MAC) address, the International Mobile Equipment Identifier (IMEI), or Mobile

Equipment Identifier (MEID)), mobile network information of devices used by **Subject Account** in conjunction with the service.

f. contact lists or images Snapchat has obtained from devices used by the **Subject Account** respectively.

g. receipts for any transactions conducted by the **Subject Account** respectively.

h. content of all communications, including Snaps, Stories, or Chats, sent or received by **Subject Account**.

III. Information to be Seized by Law Enforcement Personnel

All information described above in Section II that constitutes evidence and instrumentalities of violations of Title 21, United States Code, Section 846 involving the **Subject Account**:

- a. Snapchat username;
- b. Email address;
- c. Phone number;
- d. Display name;
- e. Snapchat account creation date and IP address;
- f. Timestamp and IP address of account logins and logouts (may also include device information);
- g. Device information and device history;
- h. Purchase history (information about services and items purchased through Snap, including in-app purchases, custom filters, and lenses -- includes what was purchased and date of purchase);
- i. Account change history (a log of changes to the account made by the user, including dates/times of changes in registration email address or phone number, birthdate, and display name);
- j. Whether account phone number has been verified;
- k. Last Active date;
- l. Whether Maps is enabled;

- m. Whether two-factor-authentication is enabled;
- n. App version;
- o. Logs containing metadata about a user's Snaps, Stories, Chats;
- p. Associated accounts;
- q. Additional user profile data, including number of Stories viewed; "discover channels" viewed; and ads, apps, and websites that the user has interacted with;
- r. Subscriptions (the accounts/"discover channels" to which a user has "subscribed" (generally, content from brands, news organizations, corporate entities, or influencers));
- s. Friends (overview of the user's friends, the friend requests sent, and users blocked and deleted);
- t. Location data (for users who have turned on location service and opted into location services in the app settings) – including frequent locations, latest locations, top locations, and locations the user has visited;
- u. Memories content (until deleted by a user);
- v. Encrypted My Eyes Only content (Snap can provide the data file but cannot decrypt it);
- w. Search history;
- x. "Our Story" and Crowd-Sourced Content (content that the user submitted to Snap's curation team);
- y. Snap History (basic information about Snaps the user has recently sent and received, including the sender, recipient, type of Snap, and date). Because of Snap's retention policy, this information is likely to be extremely limited;
- z. Snap survey responses/results.

ADDENDUM TO ATTACHMENT B

With respect to the search of any information and records received from the social media company, law enforcement personnel will locate the information to be seized pursuant to Section III of Attachment B according to the following protocol.

The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. searching for and attempting to recover any hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein.
- b. surveying various file directories to determine whether they include data falling within the list of items to be seized as set forth herein.
- c. opening or reading portions of files and records, in order to determine whether their contents fall within the items to be seized as set forth herein, and/or
- d. performing key word searches through all records to determine whether occurrences of language contained in such records exist that are likely to appear in the information to be seized described in Section III of Attachment B.

Law enforcement personnel are not authorized to conduct additional searches on any information beyond the scope of the items to be seized by this warrant.